Cisco Secure Firewall

네트워크와 보안

보안 컨트롤

일관적인 정책과 가시성

네트워크 전체를 보안 아키텍처의 일부로 바꿔보세요

비즈니스에 중요한 애플리케이션은 클라우드와 온프레미스 기반이 섞여 있고 사용자는 어디서나 리소스에 안전하게 액세스해야 하기 때문에, 기존의 방화벽 전략으로는 더 이상 효과를 볼 수 없습니다. 시스코의 단일 네트워크 경계는 여러 개의 마이크로 경계로 진화했습니다.

많은 조직에서 애플리케이션 새로운 경계가 되고, 기존 방화벽 배포가 물리적, 가상적, 클라우드 네이티브 어플라이언스로 진화하게 되었습니다.

그 결과, 현대적 애플리케이션 환경에 대한 지원을 운영화하는 데 어려움을 겪고 있습니다. 조직을 위험에 노출시키는 취약성을 공개하지 않고 일관적인 가시성과 정책 적용, 균일한 위협 가시성을 유지하는 방법을 알아내기가 어렵습니다.

시스코에서는 네트워크 보안 비전인 NetWORK를 통해 애플리케이션과 점점 더 이질적으로 되어가는 네트워크에서 정책과 적용을 조화시킬 수 있는 더욱 민첩하고 자동화된 통합 전략을 지원하고자 합니다.

Secure Firewall은 코어 네트워킹 기능과 네트워크 보안을 가장 심층적으로 통합하여 그 어느 때보다도 가장 안전한 아키텍처를 제공합니다. 이를 통해 모든 곳에서 애플리케이션과 사용자를 보호하는 완전한 보안 포트폴리오가 완성되었습니다.

장점

- 모든 애플리케이션 환경에서 통합적 제어를 제공하기 위한 실시간 통합 워크로드와 네트워크 보안
- 중요한 소스의 인텔리전스를 활용 및 공유하는 네트워크 보안 플랫폼 전략을 통해 탐지, 대응, 복구 업데이트 속도를 높이고 원격 보호 지원

  매우 안전한 기업에서 일하는 직원은 조직, 사용자, 중요한 애플리케이션을 보호하는 강력한 위협 방지 기능이 적용된 상태에서 언제, 어디서나 모든 기기에서 액세스합니다.
- 모든 Cisco Secure Firewall에 포함된 SecureX 제품은 모든 Cisco Secure 포트폴리오에서 위협의 상관관계를 알 수 있는 긴밀한 보안 통합 전략을 제공하고 대응을 가속화합니다.

The bridge to possible

시스코를 선택해야 하는 이유

Cisco Secure Firewall 포트폴리오는 점점 진화하고 복잡해지는 위협에 대해 더욱 강력한 네트워크 보호를 제공합니다. 시스코를 사용하면 민첩하고 통합적인 보안의 기반을 마련하고 현재와 미래에 누구보다도 강력한 보안 태세를 갖추는 데 투자하는 것과 같습니다.

데이터 센터, 지점 사무실, 클라우드 환경 등을 비롯한 모든 곳에서 시스코 제품과 서비스로 기존 네트워크 인프라를 확장 솔루션의 연장으로 바꾸고, 필요한 모든 곳에서 세계적 수준의 보안 컨트롤을 구현할 수 있습니다.

지금 Secure Firewall 어플라이언스에 투자하면 암호화 트래픽을 검사할 때 발생하는 성능 저하 없이, 아무리 지능적인 위협이라도 강력하게 차단할 수 있습니다. 또한, 다른 시스코 및 타사 솔루션과 결합하면 광범위하고 깊이 있는 보안 포트폴리오 제품이 모두 함께 작동하면서 원래 분리되어 있었던 이벤트의 상관관계를 찾아내고 노이즈를 제거해 위협을 더욱 빠르게 차단합니다.

보안 컨트롤

위협은 더욱 지능화되었고 네트워크는 더욱 복잡해졌습니다. 최신 상태를 유지하면서 끊임없이 새로 나타나고 진화하는 위협을 성공적으로 차단하기 위한 리소스를 갖춘 조직은 없고, 있더라도 매우 극소수에 불과합니다.

위협과 네트워크가 점점 복잡해지면서 데이터, 애플리케이션, 네트워크를 보호하는 데 적절한 도구를 갖추는 것이 중요하게 되었습니다. Cisco Secure Firewall은 위협에서 한발 앞서 나가는 데 필요한 기능과 유연성을 제공합니다. 고유한 하드웨어 기반의 암호화 트래픽을 대규모로 조사하는 기능을 제공할 뿐만 아니라, 이전 세대 애플리케이션에 비해 성능이 무려 3배나 향상되었습니다. 또한, Snort 3 IPS의 인간이 읽을 수 있는 규칙은 보안, eDynamic 애플리케이션 가시성을 단순화하는 데 도움을 주고

Cisco Secure Workload 통합을 통한 제어를 제공하여 모든 네트워크와 워크로드에서 요즘의 가장 최신 애플리케이션을 일관적으로 보호합니다.

고객 사례 | 동영상 보기

일관적인 정책과 가시성

Secure Firewall 포트폴리오를 사용하면 미래에 대비한 유연한 관리까지 포함된 더욱 강력한 보안 태세를 갖출 수 있습니다. 시스코는 기술과 비즈니스 요구 사항에 맞는 다양한 관리 옵션을 제공합니다. 예를 들어 Firewall Device Manager(FDM), Cisco Secure Firewall Management Center(FMC), Cisco Defense Orchestrator(CDO) 및 Cisco Security Analytics and Logging이 있습니다.

Cisco FDM은 로컬에서 소규모 배포를 관리하는 온디바이스 관리 솔루션입니다. Cisco Secure FMC는 보안 이벤트와 정책을 중앙에서 관리하고 자세한 보고 및 로컬 로깅을 제공하는 대규모 배포용 온프레미스 솔루션입니다. CDO는 확장된 네트워크에서 보안 정책과 기기 관리를 간소화하는 클라우드 기반 보안 관리자입니다. Cisco Security Analytics and Logging은 행동 분석을 통해 확장 가능한 로그 관리를 제공합니다.

고객 사례 | 동영상 보기

Cisco Secure Firewall의 고급 기능:

고급 기능	상세 정보
Cisco Secure Workload 통합	• Cisco Secure Workload (Tetration)를 통합하면 모든 네트워크와 워크로드에서 분산되고 동적인 요즘의 애플리케이션에 대한 포괄적인 가시성을 얻고 정책을 적용할 수 있으며, 따라서 확장 가능한 방식으로 일관적인 적용이 가능합니다.
Cisco Secure Firewall Cloud Native	• Kubernetes를 기반으로 AWS에서 가장 먼저 운영을 시작한 Secure Firewall Native Cloud는 매우 탄력적인 클라우드 네이티브 인프라를 구축할 수 있으면서도 개발자에게 편리한 애플리케이션 액세스 솔루션입니다.
동적 정책 지원	• 동적 속성은 고정 IP 주소를 사용할 수 없는 경우에 VMware, AWS, Azure 태그를 지원합니다. • 시스코는 Security Group Tag(SGT)와 Cisco Identity Services Engine(ISE) 속성 지원으로 태기 기반 정책의 시대를 열었습니다.
Snort 3 차세대 침입 예방 시스템	• 업계 최고의 오픈 소스 Snort 3로 위협을 탐지하면 탐지 기능을 개선하고, 맞춤화를 단순화하고, 성능을 개선하는 데 도움이 됩니다.
Transport Layer Security (TLS) 서버 ID 및 발견	• 암호화된 TLS 1.3 트래픽에서 레이어 7 정책을 유지할 수 있습니다. 모든 트래픽 플로를 복호화해서 검사하는 것이 불가능한 암호화 시대에 맞는 주요 가시성과 컨트롤을 제공합니다. 서로 상충하는 방화벽은 암호화된 TLS 1.3 트래픽에서 레이어 7 정책이 제대로 적용되지 않습니다.
Secure Firewall Management Center (FMC)	• 방화벽, 애플리케이션 제어, 침입 방지, URL 필터링, 멀웨어 방어 정책을 통합 관리합니다. • Cisco Secure Workload(구 Tetration)와 통합하면 네트워크와 워크로드에서 사용하는 동적 애플리케이션에 일관적인 가시성을 제공하고 정책을 적용할 수 있습니다.
Cisco Defense Orchestrator CDO	• Cisco Secure Firewall에서 일관적이고 쉽게 정책을 관리하는 데 도움이 되는 클라우드 기반 방화벽 관리입니다.
Cisco Security Analytics and Logging (SAL)	• 매우 확장성이 좋은 온프레미스 겸 클라우드 기반 방화벽 로그 관리 제품으로, 동작 분석으로 위협을 실시간 탐지하고 대응 시간을 단축합니다. 또한, 지속적인 분석을 통해 보안 태세를 추가로 다듬어서 미래의 공격 시도에 대한 방어를 강화합니다. • 모든 Cisco Secure Firewall에서 로그 집계로 규정을 준수하실 수 있습니다. • 방화벽 관리자를 긴밀히 통합하여 광범위한 로깅과 분석을 제공하며, 하나의 직관적인 뷰에서 방화벽 로그 데이터를 집계합니다.
SecureX 플랫폼	• SecureX 플랫폼을 사용하여 위협 탐지와 복구 업데이트를 가속화합니다. 모든 Secure Firewall에는 Cisco SecureX 사용권이 포함됩니다. Firewall Management Center의 새로운 SecureX 리본을 사용하면 SecOps가 SecureX의 오픈 플랫폼으로 바로 전환하여 신속하게 인시던트에 대응할 수 있습니다.
Advanced threat intelligence (Talos)	• Cisco Talos Intelligence Group은 세계에서 가장 규모가 큰 상업적 위협 인텔리전스 팀입니다. 이들은 정확하고, 빠르고 실천 가능한 위협 인텔리전스를 생성해 시스코 고객, 제품, 서비스에 제공합니다. Talos는 Snort.org, ClamAV 및 SpamCop의 공식 규칙 세트를 관리합니다.

다음 단계

Secure Firewall에 대한 자세한 정보는 http://cs.co/9007MxYrS를 확인하세요.
구매 옵션을 확인하고 시스코 영업 담당자와 상담하려면 여기를 방문하세요.

C45-736624-04